Mobile Device Encryption Policy

# Overview

Mobile devices such as smart phone and tablets offer great flexibility and improved productivity for employees. However, they can also create added risk and potential targets for data loss. As such, there use must be in alignment with appropriate standards and encryption technology should be used when possible.

# Purpose

This document describes Information Security's requirements for encrypting data at rest on <Company Name> mobile devices.

# Scope

This policy applies to any mobile device issued by Company\_A or used for Company\_A business which contains stored data owned by Company\_A.

# Policy

All mobile devices containing stored data owned by Company\_A must use an approved method of encryption to protect data at rest. Mobile devices are defined to include laptops, PDAs, and cell phones.

Users are expressly forbidden from storing Company\_A data on devices that are not issued by Company\_A such as storing Company\_A email on a personal cell phone or PDA.

* 1. **Laptops**

Laptops must employ full disk encryption with an approved software encryption package. No Company\_A data may exist on a laptop in plaintext.

* 1. **PDAs and Cell phones**

Any Company\_A data stored on a cell phone or PDA must be saved to an encrypted file system using Company\_A approved software. Company\_A shall also employ remote wipe technology to remotely disable and delete any data stored on a Company\_A PDA or cell phone which is reported lost or stolen.

* 1. **Keys**

All encryption keys and pass-phrases must meet complexity requirements described in Company\_A’s *Password Protection Policy*.

* 1. **Loss and Theft**

The loss or theft of any mobile device containing Company\_A data must be reported immediately.

# Policy Compliance

* 1. Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

# Exceptions

Any exception to the policy must be approved by the Infosec Team in advance.

# Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

# Related Standards, Policies and Processes

* Password Protection Policy

# Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at:

https://www.sans.org/security-resources/glossary-of-terms/

* Plaintext
* Full Disk Encryption
* Remote Wipe

# Revision History

|  |  |  |
| --- | --- | --- |
| **Date of Change** | **Responsible** | **Summary of Change** |
| Dec 2013 | SANS Policy Team | Converted format and retired. |
|  |  |  |